Amendments to the Specification:

Please amend the specification as follows:

Please replace paragraph starting at pages 4-5, with the following rewritten paragraph:

Variants of the CBC and XOR schemes are proved to be confidentiality-secure against chosen-plaintext attacks. For example, M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, in "A Concrete Security Treatment of Symmetric Encryption," Proceedings of the 38th Symposium on Foundations of Computer Science, IEEE, 1997, pp. 394-403, demonstrate that the CBC and XOR schemes are secure in the left-or-right (or real-or-random) sense, which in turn implies that they are confidentiality-secure against chosen-plaintext attacks (viz., S. Goldwasser and M. Bellare: "Lecture Notes on Cryptography," 1999, available at www-cse.ucsd.edu/users/mihir/papers/gb.pdf ~~http://www-cse.ucsd.edu/users/mihir/papers/gb.pdf~~). Similarly, those skilled in the art can easily show that other schemes, such as PCBC and "infinite garble extension" schemes, are also confidentiality-secure against chosen-plaintext attacks. However, not all schemes for the encryption of multi-block data or messages are confidentiality-secure against chosen-plaintext attacks. For example, it is well known in the art that the Electronic Codebook (ECB) mode of encryption (viz., NBS FIPS Pub 81, titled "DES Modes of Operation," National Bureau of Standards, U.S. Department of Commerce, December 1980) is not confidentiality-secure against chosen-plaintext attacks (viz., S. Goldwasser and M. Bellare: "Lecture Notes on Cryptography," 1999, available at www-cse.ucsd.edu/users/mihir/papers/gb.pdf ~~http://www-cse.ucsd.edu/users/mihir/papers/gb.pdf~~).

Please replace paragraph starting at page 6, with the following rewritten paragraph:

Encryption schemes that require two sequential passes over the data or message and use only one cryptographic primitive, and those that use two cryptographic primitives sequentially, to provide integrity of encrypted messages or data (1) decrease the performance of message and data encryption considerably, and (2) cannot be applied to real-time

applications where commencing verification of message integrity cannot be deferred until the end of message decryption (viz., E. Petrank and C. Rackoff: "CBC MAC for Real-Time Data Sources," DIMACS Technical Report, TR 97-26, Rutgers University, New Brunswick, N.J.; manuscript also available at www.cs.technion.ac.il/~erez/publications.html ~~http://www.cs.technion.ac.il/~erez/publications.html~~, 1999). Furthermore, schemes using one cryptographic primitive and two processing passes concurrently, and those using the two cryptographic primitives concurrently, can achieve high-performance for confidentiality and integrity but require substantial implementation complexity, cost, and additional power, and are less suitable for implementation in low-power applications, and low-power, low-cost hardware devices.